Testimony of Stephen Poorman
International EHS Manager
FUJIFILM Imaging Colorants Ltd.

on behalf of the

Society of Chemical Manufacturers and Affiliates

before the

Subcommittee on Energy & the Environment

of the

U.S. House of Representatives
Committee on Energy & Commerce

on

The Chemical Facility Anti-Terrorism Act of 2009 (H.R. 2868)

October 1, 2009

Good morning, Chairman Markey, Ranking Member Upton, and members of the Subcommittee. My name is Stephen Poorman, and I am the International Environment, Health & Safety Manager for FUJIFILM Imaging Colorants Ltd. I am pleased to provide this testimony regarding H.R. 2868, the "Chemical Facility Anti-Terrorism Act of 2009." I speak before you today on behalf of the Society of Chemical Manufacturers and Affiliates (SOCMA), of which FUJIFILM is a member.

Americans recently observed the ninth anniversary of 9/11. Three short years ago, and working in a bipartisan manner, Congress enacted a strong chemical security regulatory program that was finally in place on that painful day of remembrance. The U.S. Department of Homeland Security (DHS) and thousands of regulated facilities are deep in the middle of implementing this vital program in a focused, cooperative manner. We urge you not to upset – and further delay – this important process by sending DHS and regulated facilities back to the drawing board.

SOCMA strongly supports DHS's current Chemical Facility Anti-Terrorism Standards (CFATS) program. This demanding program is now requiring thousands of chemical facilities nationwide to develop and deploy meaningful security enhancements. Congress should reauthorize the underlying statute for another year, or simply make the current program permanent.

In large measure, H.R. 2868 essentially codifies the existing CFATS program, and SOCMA supports it to that extent. However, the bill contains several features that are fundamentally unwise and potentially counterproductive to our shared goal of preventing terrorist incidents at chemical facilities. After sharing with you what steps SOCMA and its members have taken before and within the CFATS program, I will explain why we respectfully, but strongly, oppose:

- Any mandate that facilities implement so-called inherently safer technology ("IST"); and
- A citizen suit provision in chemical facility security legislation.

I. SOCMA and the Current State of Chemical Facility Security

SOCMA

SOCMA is the leading trade association representing the batch and custom chemical manufacturing industry. SOCMA's nearly 300 member companies employ more than 100,000 workers across the country and produce some 50,000 products – valued at $60 billion annually – that make our standard of living possible. From pharmaceuticals to cosmetics, soaps to plastics and all manner of industrial and construction products, SOCMA members make materials that save lives, make our food supply safe and abundant, and enable the manufacture of literally thousands of other products. Over 70% of SOCMA's active members are small businesses.

ChemStewards® is SOCMA's flagship environmental, health, safety and security (EHS&S) continuous performance improvement program. It was created to meet the unique needs of the batch, custom, and specialty chemical industry, and reflects the industry's commitment to reducing the environmental footprint left by members' facilities. As a mandatory requirement for SOCMA members engaged in the manufacturing or handling of synthetic and organic chemicals, ChemStewards is helping participants reach for superior EHS&S performance.

SOCMA's Security Achievements to Date

Maintaining the security of our facilities has always been a priority for SOCMA members, and was so before September 11. After the tragic events of 9/11, SOCMA members did not wait for new government regulations before researching, investing in and implementing additional and far-reaching facility security measures to address these new threats. Under the ChemStewards initiative, SOCMA members were required to conduct security vulnerability assessments (SVAs) and to implement security measures. SOCMA designed an SVA methodology specifically for specialty and batch chemical facilities that was approved by the Center for Chemical Process Safety (CCPS) as meeting its requirements for an effective methodology. SOCMA members have spent billions of dollars and have devoted countless man-hours to secure their facilities and operations. These investments will naturally continue for the foreseeable future.

Many (though by no means all) SOCMA member company facilities are encompassed by the CFATS program. These facilities have completed and submitted their Top-Screens and SVAs and, as notified by DHS, have initiated or completed their Site Security Plans. These plants are implementing any additional required security measures and are being (or will soon be) inspected by DHS to verify the adequacy of those plans and their conformance to them. Many of our member companies' other facilities comply with the Coast Guard's facility security requirements under the Maritime Transportation Security Act (MTSA).

Looking well beyond regulatory requirements, our members have also partnered with DHS on many important voluntary security initiatives and programs, including the Risk Assessment Methodology for Critical Asset Protection (RAMCAP), the Buffer Zone Protection Plans, and the Homeland Security Information Network (HSIN). SOCMA is a key member of the Chemical Sector Coordinating Council, which has served as a model for how critical infrastructure sectors should work together and with DHS.

Through these councils and other avenues, we and our members have developed close and open working relationships with DHS and other federal agencies, and with state and local governments, to exchange information and coordinate roles in maintaining the security of our critical chemical facility infrastructure. These actions have included holding joint training exercises and conducting annual security conferences that involve federal and state government officials with security expertise. Industry personnel from the largest companies to the smallest have shared best practices at association meetings and conferences.

Preserving the Progress under CFATS

While we will leave a detailed progress report on the CFATS program to DHS, SOCMA wants to emphasize that we regard the program thus far as a success. Almost 40,000 facilities have submitted Top-Screens, close to 7,000 have completed SVAs, and DHS has now requested SSPs from three of the four tiers of facilities under the program. Tier 1 SSPs are being actively reviewed and inspections will follow soon. Of perhaps greatest interest to many members of this panel, we understand that some 600 facilities – roughly 10 percent of the initial Top-Screen population- have changed processes or inventories in ways that have enabled them to screen out of the program. Thus, as predicted, CFATS is driving facilities to reduce inherent hazards, where doing so is in fact safer and does not transfer risk to some other point in the supply chain, and makes economic sense.

To fully understand the effectiveness of the CFATS program, Congress should allow it to be fully implemented – for all tiered facilities to fully comply (or be brought into compliance). Thus, Congress should reauthorize the underlying statute for another year or simply make the current program permanent.

Two provisions of H.R. 2868 would jeopardize the progress that industry and DHS have made together under CFATS. First, the requirement for mandatory implementation of IST would shift DHS's focus from securing our industry against terrorism to conducting engineering and chemistry assessments, while potentially phasing out legitimate products that improve our daily lives and enhance our safety. Second, the citizen suit provision would promote litigation that would increase security risks through the advertent or inadvertent disclosure of sensitive security-related information that could draw a roadmap for terrorists. Each of these concerns is explained in greater detail below.

II. Mandatory IST Is an Inherently Risky Proposition

As established by H.R. 2868, Section 2111 of the CFATS statute would require Tier 1 and 2 facilities to implement "methods to reduce the consequences of a terrorist attack" – i.e., IST – whenever DHS made specified findings about risk reduction and technical and economic feasibility. However commonsense such a mandate might appear on the surface, it is fundamentally a bad idea in the security context. Inherent safety is a superficially simple but truthfully very complex concept, and one that is inherently unsuited to regulation. Any IST mandate is bound to create situations that will *actually increase or transfer overall risks*. It would also wreak economic havoc on regulated facilities, notwithstanding the findings DHS would have to make. Makers of active pharmaceutical ingredients, common fuels and other federally-regulated substances would be most at risk of such economic damage.

What Inherent Safety Really Is and Why Mandating It Is Not Inherently Better

First and foremost, it is important to clarify a common misunderstanding about inherent safety. Quite simply, IST is a process-related engineering concept, not a security one. It is premised on the belief that, if a particular chemical process hazard can be reduced, the

overall risk associated with that process will also be reduced. In its simplicity, it is an elegant concept, but reality is almost never that simple. A reduction in hazard will reduce overall risk if, and only if, that hazard is not displaced to another time or location, or result in the creation of some new hazard. Inherent safety is only successful if the sum total of all risks associated with a process life cycle is reduced. This is rarely a simple calculation, and to some extent it is an irreducibly subjective one (for example, a substitute chemical that may reduce explosion risks may also pose chronic health risks). The calculation becomes even more difficult when it is being done not solely for reasons of process safety (where accident probabilities can be estimated with some degree of confidence) but also for reasons of security (where the probability of terrorist attack is highly uncertain but certainly low). In fact, there is no agreed-upon methodology to measure whether one process is inherently safer than another process. This is why the world's foremost experts in IST and chemical engineering consistently recommend against regulating inherent safety for security purposes.

Several examples of how difficult it can be to reduce overall risk when attempting to reduce hazard follow:

Eliminating the use of a hazardous catalyst

A chemical company wants to eliminate the use of a hazardous catalyst, which is typically used in small amounts. The catalyst serves as a booster to start a chemical reaction to make a building block for a drug used to treat cancer. Catalysts tend to be hazardous by nature, which reduces the number of available alternatives. The only way the company can initiate the reaction without using a hazardous catalyst is to increase the temperature and pressure of the system. The overall risk of the new system, aggravated by increasing the temperature and pressure, may actually be greater than the risk associated with use of the catalyst, because catalysts are typically used in small amounts and the likelihood of an accident is remote.

Reducing the amount of a chemical stored on site

A manufacturing plant is considering a reduction in the volume of a particular chemical stored on site. The chemical is used to manufacture a critical nylon additive, which is sold to another company and used to make seat belts stronger. Because it is a critical component for nylon strength and seatbelt production cannot be disrupted, the production schedule cannot change. If the amount stored on site is reduced, the only way to maintain the production schedule is to increase the number of shipments to the site. This leads to more deliveries (an increase in transportation risk) and more transfers of chemical from one container to another (an increase in transfer risk). Economic risks are also increased since there is now a greater chance that production could be disrupted by a late shipment.

How location and individual circumstance affect risk perception

It is difficult to describe a scenario in which moving a hazard does not result in a simple transfer of risk from one location to another. For example, location can highlight different

risk perspectives, such as the use of chlorine, a hazardous gas that comes in various types of containers. A commonly used example compares the inherent safety of a rail car, which typically holds up to 90 tons, versus storage in one-ton cylinders. Residents near the facility would probably view the one-ton cylinder as inherently safer than a rail car. On the other hand, workers who have to connect and disconnect the cylinders 90 times, instead of just once for the rail car, would probably consider the rail car inherently safer.

IST's Impact on Pharmaceuticals and Microelectronics

One of SOCMA's greatest concerns with Section 2111 is the real possibility that it will negatively restrict the production of active pharmaceutical ingredients (APIs), many of the key raw materials of which are included on DHS's Appendix A of covered chemicals. APIs are used in prescription and generic drugs, life saving vaccines and over-the-counter medicines. They are thoroughly regulated by the FDA and must meet demanding quality and purity requirements. Substituting chemicals or processes used for the production of APIs would likely violate the conditions of their FDA approvals. Requiring IST could delay clinical trials while new replacement chemicals are identified or invented, and would force API manufacturers and their customer drug manufacturers to reapply for FDA approval of their products because of the significant change in the manufacturing.[1] The lengthy 1 - 4 year approval timeline for a new or equivalent replacement chemical would be a high price to pay for American consumers, many of whom rely on ready access to pharmaceuticals. To meet continuing consumer demand, API production would likely shift to foreign countries, where the FDA is less able to monitor conformance to quality standards.

Many SOCMA members' products are also vital to the manufacture of microelectronics. Below, we offer several examples, provided by SOCMA members, of how IST could cripple the pharmaceutical and microelectronics industries.

Lifesaving Antibiotics: Company A

Company A is a minority-owned small business regulated by DHS under CFATS. It produces an active pharmaceutical ingredient critical to specific antibiotics used in the treatment of a life-threatening bacterial infection. For this purpose, the company is also regulated by the FDA. Since the product's specifications are likely not to be attainable via any chemical substitution or altered process, if a "safer" manufacturing process alternative was mandated, the company would likely be forced to discontinue production, lay off workers and increase our nation's vulnerability to bacteriological threats. The impact of a mandatory alternative would thus be swift and direct.

Common Pain Reliever: Company B

Company B manufactures the active pharmaceutical ingredient Ibuprofen. Ibuprofen is a non-steroidal anti-inflammatory drug (NSAID) used to treat pain and relieves symptoms

[1] *See* 21 U.S.C. § 351(a)(2)(B).

of arthritis such as inflammation, swelling, stiffness, and joint pain. It is one of the world's most successful and widely-used pain relievers, and is listed on the World Health Organization's model list of medicines.[2] Changing the raw materials, and consequently the process, used to manufacture it presents a risk to public health and a substantial cost for re-qualification from a technical, regulatory, and potentially clinical perspective. Company B's 31-year old process to manufacture Ibuprofen bulk active is well characterized and controlled, and consistently makes a safe and efficacious product. The process-characteristic impurity profile, specified under the prevailing USP and European Pharmacopoeia compendia, is proven to have no impact to public health by its use by millions of people worldwide. The costs derived from IST, if it impaired production quantities or product quality, would ultimately be felt by consumers.

Microelectronics: Company C

Company C manufactures two Appendix A chemicals of interest targeted by industry critics. First, Company C uses small amounts of hydrochloric acid (HCl) in a very high purity, aqueous form (37%) to manufacture a product that represents almost half of the company's revenue worldwide (~$30 million/yr). The product is used in the microelectronics industry to manufacture integrated circuits and LCD displays. If HCl were not available, Company C would be unable to make its largest product, resulting in at least a 50% reduction in workforce, which would equate to losing 60 jobs. If the company chose to continue the business, alternatives would have to be developed and implemented to continue manufacture of those products, which could easily require billions of dollars of research, development and implementation, resources that small companies like Company C, which include many of SOCMA's members, do not have. Additionally, Company C uses HCl to protect the environment: its use brings the pH of the company's wastewater into the range dictated by its wastewater permit.

The company also uses small volume products using aqueous (49%) hydrofluoric acid (HF) that are sold into the microelectronics industry. Customers of Company C that need HF for their products require Company C to undergo specific certification standards as a product supplier. If Company C was forced to use a substitute, it would immediately be out of compliance with its customers' product standards, which (obviously) would negatively impact Company C's business. In some cases, the HF is being used as a safer alternative to replace hydroxylamine (HA), the use of which has been reduced due to the multiple explosions at HA manufacturing facilities. In some cases, anhydrous HF may be necessary as water may be incompatible with the manufacturing process. If manufacturers of microelectronics were denied a supply of HF, there would be a negative consequence to the domestic manufacture of integrated circuits and LCD displays.

Experts Agree IST Should Not Be Mandated

As these examples demonstrate, a "simple" reduction in hazard may not necessarily result in a reduction of overall risk, and a poorly constructed or incomplete analysis could result

[2] World Health Organization, *WHO Model List of Essential Medicines* (March 2005).

in a "safer" alternative producing more harm than good. That is why government agencies and experts who really understand inherent safety have consistently opposed giving government the power to mandate it. This includes:

- Neal Langerman, representing the American Chemical Society – the majority's own technical witness at the Homeland Security Committee hearing in June.[3]
- Sam Mannan, Director of the Mary Kay O'Connor Process Safety Center at Texas A&M University, in testimony before the Homeland Security Committee on December 12, 2007.[4]
- Dennis Hendershot, testifying on behalf of the Center for Chemical Process Safety before the Senate Environment & Public Works Committee on June 21, 2006.[5]

---

[3] *See* http://homeland.house.gov/SiteDocuments/20090616103505-95857.pdf, page 7:

> In conclusion, the existing regulatory structure, under the U.S. EPA Risk Management program and the U.S. OSHA Process Safety Management standard, provide strong incentives to examine and implement IST. These programs work in natural conjunction with Homeland Security's mandate to enhance infrastructure security. The provisions of the Chemical Facility Antiterrorism Act of 2006 provide a sufficient legislative framework for this purpose. The most effective steps to further infrastructure protections will likely include incentives, rather than new regulations.

[4] Go to http://homeland.house.gov/Hearings/index.asp?ID=108, click on "Dr. Mannan's testimony," pp. 6-7:

> [I]n developing inherently safer technologies, there are significant technical challenges that require research and development efforts. These challenges make regulation of inherent safety very difficult. . . . Instead of prescriptive requirements for inherently safer technology and approaches, facilities should be allowed the flexibility of achieving a manageable level of risk using a combination of safety and security options. . . . Over the past 10-15 years, and more so after 9/11, consideration of Inherently Safer Technology (IST) options and approaches has effectively become part of industry standards, with the experts and persons with know-how assessing and implementing inherently safer options, without prescriptive regulations that carry risks (both as trumping other tools or potentially shifting risk). A better approach for applying IST in security is by allowing the companies to assess IST as part of their overall safety, security and environmental operations and therefore, cannot be prescriptive.

[5] *See* http://epw.senate.gov/109th/Hendershot_Testimony.pdf, at 4-8, esp. 5-6:

> There are tens of thousands of chemical products manufactured, most of them by unique and specialized processes. The real experts on these technologies, and on the hazards associated with the technology, are the people who invent the processes and run the plants. In many cases they have spent entire careers understanding the chemistry, hazards, and processes. They are in the best position to understand the best choices, rather than a regulator or bureaucrat with, at best, a passing knowledge of the technology.

It is likewise instructive that the state of New Jersey, whose chemical facility security program is regularly contrasted with the CFATS program, only requires consideration of IST – *it does not require facilities to implement it*. It is even more telling that the companion bill the Subcommittee is now considering avoids the politically sensitive question of whether to require public drinking water systems to implement IST by deferring the decision to EPA and the states.[6] Congress should not require DHS to do what all these experts have concluded is unwise, and what it is unwilling to do directly when the public is picking up the tab.

Conditioning the IST Mandate on "Key Criteria" Does Not Solve the Problem

SOCMA is aware that the Administration now supports mandating IST for Tier 1 and 2 facilities when unspecified "key criteria" are met. But that approach does not address our fundamental objections to the concept, which is that it would take IST decisions away from the process safety experts who know their own processes the best and would allow their judgments to be second-guessed by busy government officials sitting miles away reviewing documents. While these officials may be sincerely trying to do their best, we simply do not trust that their judgments will be better than ours. We also fear the prospect of liability if a "safer" process or chemical that one of our member companies is compelled to use ends up causing an accident or some other harm. Will the federal government indemnify facilities in the cases where it overrules their judgments regarding inherent safety? And even if a facility ultimately succeeds in persuading DHS to allow it to retain its proposed approach, that process will inevitably have costs in time and resources.

Preceding all these concerns, moreover, is an even more basic one: no one knows how to compare the "inherent safety" of two processes. Here is what the experts have told Congress:

- I do not believe that the science currently exists to quantify inherent safety. . . . The first challenge is simply to measure the degree of inherent safety in a way that allows comparisons of alternative designs . . . .[7]

- Inherently safer design is not a specific technology or set of tools and activities at this point in its development. . . . Current books and other literature on inherently safer design . . . describe a design philosophy and give examples of implementation, but do not describe a methodology.[8]

- While scientists and engineers have made great strides in understanding the impacts of industrial processes and products over the past several decades, there is still no

[6] *See* 42 U.S.C. § 300i-2(g)(3), (5), as proposed to be modified by H.R. 3258, § 2(a).
[7] Testimony of Sam Mannan, *supra* note 4, at 6.
[8] Testimony of Dennis Hendershot, *supra* note 5, at 1-2.

guaranteed formula for developing inherently safer production processes.[9]

The experts at the National Research Council concluded recently: "Inherently safer chemistry . . . offers the potential for improved safety at chemical facilities. While applications show promise and have found use within the chemical industry, these applications at present are still quite limited in scope."[10]

While it may be feasible to develop a technical consensus methodology for measuring and comparing inherent safety, none exists at present. Before Congress and the Administration could even consider mandating IST implementation, they would need to know that methodologies exist to compare various alternatives from the standpoint of inherent safety. Congress should direct DHS to submit a report to it that explains in detail what methodologies DHS would propose to use. Such a report should be developed with broad participation by the expert community, most of which works for the chemical industry. This will require a year at least. It would also allow DHS to devote some time to completing its implementation of the current CFATS program, rather than being completely sidetracked by trying to regulate with concepts that even the experts do not yet agree on.

III. Citizen Suits Have No Place in a Security Regime

As revised by H.R. 2868, Section 2116 of the CFATS legislation would authorize literally "any person" to file suit against either

- anyone who the plaintiff believed was violating some requirement of the new law; or
- DHS, if the plaintiff believed that DHS had failed to take some nondiscretionary action the law required it to take.

Both of these prospects would be bad security policy, as explained below.

Facilities should not be subject to suit under H.R. 2868

Section 2116 is very closely modeled on the citizen suit provisions of environmental and natural resource statutes. One of the main reasons that citizen suit provisions are found in some such laws is because the obligations – and the compliance status – of regulated entities under them is a matter of public record. It is relatively easy to get access to facilities' permits, and their compliance data is normally also made public as a matter of law – in many cases, on the Internet. Also, citizen enforcement is generally thought to promote the purposes of these laws. By adding citizen oversight to EPA and state

[9] Testimony of Neal Langerman, *supra* note 3, at 6-7.
[10] National Research Council, Board on Chemical Sciences & Technology, *Terrorism and the Chemical Infrastructure: Protecting People and Reducing Vulnerabilities* (2006), at 106.

enforcement, Congress believes it can help eliminate or reduce emissions, discharges, etc. of pollution.

Citizen oversight of enforcement of security laws, by contrast, would actually be counterproductive to the purposes of those laws. Currently – and under H.R. 2868 – the only fact about a facility's regulation under the CFATS program that a citizen might be able to obtain legally is that fact that the facility *is* regulated. Every other item of information that the facility or DHS has developed under the law – the facility's tier level, vulnerability assessment, security plan, list of security measures, etc. – is prohibited from being released to the general public (for example, under the Freedom of Information Act), both under current law and under H.R. 2868. And for good reason: if this information were publicly available, terrorists could use that information to target the facility and its surrounding community. Because this information is protected (currently as "Chemical-terrorism Vulnerability Information" or "CVI"), there is no way that "any person" could evaluate the compliance status of a facility. Indeed, it is questionable whether such a person, relying on publicly-available information, could even form the reasonable belief regarding noncompliance that would be required to file a lawsuit in federal court under Rule 11(b) of the Federal Rules of Civil Procedure.

Because H.R. 2868 also limits routine public availability of compliance-related information, it would appear that the drafters of the bill expect that plaintiffs under Section 2116 would have to attempt to obtain information regarding noncompliance from DHS or regulated facilities through the process of pretrial discovery, presumably under protective orders.[11] To create an expectation that this could occur routinely would be misleading. Even under the more relaxed standard that the bill would create for access to "protected information" in litigation – equivalent to that now applicable to "sensitive security information" or "SSI" -- the bill would still make it fairly difficult to obtain such information. The plaintiff would have to show a need equivalent to that required currently to obtain fact work product, the plaintiff's counsel would have to complete a background check, and the court would have to issue a protective order after concluding that access to the information did not present a risk of harm.[12] SOCMA understands that courts have rarely, if ever, approved the release of SSI under this regime. It would be highly irregular for Congress to establish a presumptive right of action that could not, in many cases, ever be exercised.[13]

---

[11] *See* the Homeland Security Committee's report on H.R. 2868 (H. Rep. No. 111-205, pt. 1, July 13, 2009), at 49 (referring to the Committee's expectations regarding "information provided during such proceedings").

[12] *See* P.L. 109-295, § 525(d), referenced in new 6 U.S.C. § 2110(c).

[13] SOCMA also notes that the Report seems to promise greater protection of information than the bill itself provides, as the Report says "[t]he Committee expects that information provided during [citizen suit] proceedings should be maintained in accordance with existing protections for classified and sensitive materials including but not limited to the protections set forth in Section 2110 of this title." Report at 49 (emphasis added).

On the other hand, if the drafters of the bill expect that it *will* lead to wide access to protected information in citizen suits, or if that is what will in fact occur, SOCMA is even more concerned. We simply do not trust that the information protection regime established under the bill will operate successfully if it is routinely allowing security-sensitive information to be released under protective orders. These cases are likely to be so politicized, and so high-profile, that sensitive information is bound to leak out. Congress should not create weak spots in the web of applicable legal protections that could allow CVI to be disclosed in random citizen suits. Unlike the environmental laws, CFATS is one area where citizen enforcement could actually work against, not support, the protective purpose of the law.

It is for this reason that DHS Deputy Under Secretary Reitinger – a former senior DOJ official – expressed "concern" about the citizen suit provision in the Homeland Security Committee's hearing on June 16. He stated that, "no matter what the protections are," protected information "inevitably" would be disclosed over time.

Supporters of applying the citizen suit model to CFATS may argue that regulated facilities have large amounts of dangerous chemicals onsite – the same hazard that might make them regulated under environmental laws – and thus that H.R. 2868 should have the same citizen suit feature as those laws. H.R. 2868 confirms,[14] however, that it would not displace any environmental laws, and any information that a facility has to make public under those laws would remain publicly available under the bill – as it is under the current CFATS program. Citizens who want access to that information can get it, and those who think that environmental laws are not being followed at a facility can attempt to enforce those laws. But the bill should not create a litigation tool to go beyond those authorities to obtain security-related information.

Relatedly, SOCMA disputes the view, regularly asserted by proponents of a citizen suit provision, that such provisions are normal features of any federal regulatory statute. Such provisions are in fact not common: they are not contained in statutes regulating food and drugs, aviation safety, consumer product safety, bank safety & soundness, transportation safety, or any of the myriad substantive areas that the federal government regulates, aside from environment and natural resources. Nor has the Supreme Court inferred a private right of action in ages.[15] Most important, citizen suit provisions are absent from federal statutes regulating the security of ports, port facilities, vessels, aircraft, railroads, or motor vehicles. As the listing on page 49 of the Homeland Security Committee's report on H.R. 2868 (the "Report") makes clear, citizen suit provisions are exclusively an environmental/natural resources phenomenon. And chemical facility security is a security matter, not an environmental matter.

---

[14] *See* new Section 2110(d).

[15] Thus SOCMA is troubled by the Report's curious description of the citizen suit provision as "remov[ing] the current restrictions on citizen suits" from a statute that is silent on the topic. Report at 21.

DHS should not be subject to suit either

DHS has been working night and day to implement CFATS, and has developed a credible program under very tight deadlines. There is no reason to believe that DHS would have done a better job if it were acting under judicial supervision – indeed, having to defend itself in court would only distract from its ability to get the CFATS program up and running. Deputy Under Secretary Reitinger alluded to this potential for "diversion from existing labors" in his responses to questions on June 16. Again, as noted above, there is no way that average citizens should be able to determine whether DHS has acted correctly or incorrectly in approving a facility's site security plan or otherwise complying with a CFATS obligation – that information is CVI. And again, environmental laws are a bad model for a law that deals with protected, rather than public, information.

SOCMA must point out that the Report is incorrect in stating on page 49 that "the Nuclear Regulatory Commission, which, like the Department [of Homeland Security] is a security agency, is subject to suits brought by citizens." The NRC is subject to citizen suits under environmental laws in the same way as any other federal agency that operates facilities that are regulated under such laws. But the Atomic Energy Act does not authorize citizen suits against the NRC for violating or failing to take required action under the AEA. If DHS operated hazardous waste treatment plants, it would be subject to citizen suits under RCRA for its operation of those plants. But that is not a basis for saying it should be subject to suit under its own organic statute.

For these reasons, Congress should drop Section 2116 and references to it such as in proposed new Section 2108(e)(1)(D)-(F).

IV. Conclusion

SOCMA supports permanent chemical site security standards that are risk-based and realistic, and we urge Congress to reauthorize the existing CFATS program. Mandating inherently safer technology as a security measure will inevitably create negative unintended consequences, and Congress should not require DHS to do so. Citizen suits have no place in chemical facility security regulation.

On behalf of SOCMA, I appreciate this opportunity to present the association's views on these important issues. I look forward to your questions.